ZAŠTITA PRIVATNOSTI KOD VIZUELNIH INFORMACIJA U UMREŽENOM SVETU

Andreja Samčović, Nataša Tomić - Petrović,
Univerzitet u Beogradu – Saobraćajni fakultet

Sadržaj: *Pravo na privatnost već dugo predstavlja jedno od osnovnih ljudskih prava. Poslednjih tridesetak godina razvoj informacionih i komunikacionih tehnologija je doveo do ubrzanog napretka u prikupljanju, memorisanju, prenosu i razmeni ličnih informacija u javnom i privatnom sektoru. Kombinacija univerzalnih senzora, bežičnih komunikacija i metoda za prepoznavanje oblika je učinila lakšim nego ikada posmatranje svih naših dnevnih aktivnosti. Sa druge strane, korišćenje video nadzora i društvenih mreža je dovelo do sumnje u pogledu dalje upotrebe prikupljenih podataka. Kako bi se smanjila zabrinutost potrebno je razviti efikasne mehanizme u pogledu zaštite privatnosti vizuelnih informacija.*

Ključne reči: *zaštita privatnosti, video nadzor, obrada slike, društvene mreže, pravna zaštita*

1. Uvod

U umreženom društvu vizuelni mediji poseduju nove formate. Fotografije koje su ranije štampane na fotografskom papiru i memorisane u fotografskim albumima sada postoje u digitalnim formatima. Sa razvojem društvenih medija fotografski podaci se pomeraju u klaud gde im se može brzo pristupiti. Prednosti novih tehnologija se odnose na povećanu efikasnost, lakše memorisanje i smanjenu cenu distribucije. Nedostaci se ogledaju u riziku da se privatne fotografije i video zapisi koriste na način koji nije poželjan. Slike ljudi su potencijalno osetljive i sa njih se mogu očitati informacije vezane za privatne detalje o telu, načinu života, aktivnostima i još dosta drugih detalja. Osim toga, slike imaju potencijal da nepovratno unište reputaciju neke osobe [1].

Porast multimedijalnog saobraćaja preko sajtova za društveno umrežavanje, kao što su Fejsbuk i *YouTube*, uz kombinaciju savremenih tehnika za analizu multimedijalnog sadržaja, kao što su prepoznavanje lica, verifikacija govora i estimacija lokacije, dovodi do novih mogućnosti za neetičko korišćenje multimedije [2]. Prema tome, multimedijalna zajednica ima obavezu da razume rizike, istraži moguće neželjene efekte i poduči javnost u tom pogledu. Postoji mogućnost pretraživanja multimedijalnih informacija po temi, lokaciji, osobi, tipu kamere, ili vremenu, čak i ako korisnik koji je postavio te sadržaje nije eksplicitno uključio te informacije. Jednostavni metodi za anonimnost i skrivanje metapodataka više neće biti dovoljni [3].

Privatnost predstavlja pojam koji je teško definisati i koji se razlikuje u različitim kulturama. Kao posledica toga postoji veći broj definicija, kao što je, recimo, pravo da neka osoba ne bude uznemiravana. Jedna od definicija privatnosti određuje da je to "kvalitet stanja u kome neka osoba nije posmatrana od strane druge osobe ili neke organizacije", ili da je to "sloboda od neautorizovanog posmatranja". U tehničkom okruženju privatnost može da se definiše kao "praktično osiguranje od mogućih implikacija komunikacije", što se razlikuje od pojma bezbedne komunikacije, koja uključuje "osiguranje osobina komunikacije", kroz metode kriptografije, steganografije i skrivanja identiteta. Drugim rečima, zadatak istraživanja na polju privatnosti nije osiguranje komunikacionog kanala, već osiguranje da javno dostupne informacije budu samo one po odobrenju vlasnika nad sadržajima.

Dok sa jedne strane društvene mreže omogućavaju korisnicima jednostavnu razmenu fotografija, sa druge strane ih izlažu ugrožavanju privatnosti i u okviru društvenih mreža i od strane drugih entiteta. Trenutna kontrola privatnosti na društvenim mrežama je daleko od toga da je adekvatna, što rezultuje neodgovarajućim tokom informacija. Do toga dolazi bilo usled toga što korisnici nisu dovoljno pažljivi prilikom postavljanja zaštite privatnosti, bilo zbog toga što društvene mreže ne implementiraju politiku privatnosti na adekvatan način. Sajtovi za društveno umrežavanje zadržavaju pravo da analiziraju postavljene fotografije koristeći tehnike za automatsku identifikaciju lica.

Nakon uvodnog dela, u drugom poglavlju su predstavljeni potencijalni rizici po privatnost korisnika, kao i mogući napadi na privatnost, vezano za vizuelne sadržaje. Zatim su obrađene moguće metode za zaštitu privatnosti vizuelnih sadržaja, uključujući i moguću podelu tih metoda. Naredna sekcija se bavi merama pravne zaštite, imajući u vidu propise koji su posvećeni zaštiti privatnosti i sankcionisanju ugrožavanja i narušavanja privatnosti.

2. Rizici po privatnost i mogući napadi

U ovoj sekciji biće opisane tehnike za multimedijalnu analitiku koje mogu da predstavljaju potencijalne rizike po privatnost korisnika.

Estimacija lokacije - koristeći multimodalne metode, moguće je proceniti lokaciju na oko 40% video zapisa na sajtu za društveno umrežavanje *Flickr*, sa pouzdanošću od 100 m, i na preko 50% zapisa sa pouzdanošću boljom od 1 km. Ti metodi omogućavaju praćenje multimedije sa značajnim faktorom, bez uvođenja dodatnih GPS (*Global Positioning System*) senzora.

Estimacija vremena - datum i vreme se snimaju na multimedijalnom dokumentu i mogu da se procene korišćenjem lokacije Sunca ili merenjem dužine senke. Ukoliko su dva video zapisa snimljena u isto vreme i na istom mestu, i ako je poznato vreme jednog zapisa, onda je poznato i vreme drugog zapisa. Isključivanje metapodataka o vremenu i datumu sa video zapisa ne obezbeđuje zaštitu ako neko drugi ko je snimio video u isto vreme nije isključio te podatke.

Detekcija osobe - kod slika se to naziva detekcija lica, dok se kod audio signala zove prepoznavanje govora [4]. Dok korisnik koji postavlja slike može da primeni aktivne metode za anonimnost osoba koje se nalaze u prednjem delu slika, kao što je recimo zatamnjenje lica sa tamnim okvirom, privatnost osoba koje se nalaze u pozadini može da bude dovedena u pitanje [5].

Detekcija osobe - detekcija nekog skupog mobilnog uređaja može da bude znak da osoba koja ga drži bude meta napada. Stanovi mogu da budu potencijalna meta krađe zbog nameštaja koji se nalazi u pozadini nekog video zapisa. Problem kod anonimnosti je u tome što ne mogu da se uklone svi objekti sa slike, jer se onda gubi informacija o sadržaju multimedijalnog dokumenta.

Akustični šum okruženja - prilikom anonimizacije lica često se zaboravi da se ukloni akustični šum koji potiče od okruženja. Kombinacija šuma sa metodom estimacije lokacije može da dovede do značajnog narušavanja privatnosti.

Detekcija senzora - moguće je jedinstveno identifikovati koja kamera je korišćena prilikom snimanja video zapisa, na osnovu artefakata senzora. Na primer, šum piksela je jedinstven za određeni tip kamere. Detekcija senzora omogućava preskakanje postojećih metoda za anonimnost multimedijalnih informacija.

Trodimenzionalno snimanje - savremene stereo kamere imaju mogućnost snimanja i neželjenih podataka. Pošto će se taj trend samo ubrzati neophodno je da o tome multimedijalna zajednica povede računa.

Egzotični senzori - različiti senzori kao što su senzori za merenje vazdušnog pritiska, ili monitori za praćenje rada srca, postaju uobičajeni i verovatno je da će ti senzori biti uključeni u multimedijalne dokumente, kao što sada mogu da budu ugrađeni u GPS prijemnike. Budući da korisnici ne mogu uvek da imaju uvida u pouzdanost tih informacija, to znači da nemaju uticaja na zaštitu svoje privatnosti. Na primer, implikacije po privatnost vezano za geotagovanje kod GPS sistema su tek nedavno uočene.

Glavni servisi za društveno umrežavanje kao što su *Google*, Fejsbuk, Tviter, *Flickr*, *YouTube*, i *LinkedIn*, pružaju ekstenzivne aplikacije API (*Application Programming Interface*) koje čine jednostavnim automatsku pretragu multimedijalnog sadržaja. Te aplikacije imaju često sadržajniji pristup od odgovarajućeg veb interfejsa. S tim u vezi, *Google* već obezbeđuje jednostavnije forme pretraživanja slika i video zapisa i pitanje je dana kada će prepoznavanje lica postati jedan od servisa koje nudi *Google*. Fejsbuk već ima ugrađen servis za prepoznavanje lica na svojoj platformi, tako da postoji mogućnost sa drugih sajtova da pristupe prepoznavanju lica sadržaja na Fejsbuku. Mogućnosti nove generacije onlajn servisa daće novu dimenziju pitanjima privatnosti na koje društvo još nema odgovore.

Pretraživanje multimedijalnih informacija otvara široku lepezu mogućih napada na privatnost korisnika. Dok su današnje mašine za pretraživanje ograničene pre svega na tekstualne informacije, napadi mogu u skoroj budućnosti da budu usmereni ka pretraživanju audio i video sadržaja. Kriminalci mogu da povežu te sadržaje sa lokacijom potencijalnih meta. Na primer, žrtve napada mogu da budu identifikovane sa predmetima velike vrednosti i zatim da bude identifikovano kada su prazni njihovi domovi. Pretraživanje pozadine može da bude još invazivnije nego do sada.

3. Zaštita privatnosti vizuelnih sadržaja

Zaštita privatnosti se sastoji u prevenciji da informacije koje neka osoba želi da zadrži privatnim ne budu javno dostupne. U kontekstu slike i video signala to se odnosi na zaštitu vizuelne privatnosti. S tim u vezi, treba razjasniti kada nečija privatnost treba da bude zaštićena. Kada se privatnost zaštićuje treba razlikovati nečiji identitet od osetljivih

informacija koje treba da budu zadržane privatnim. Video zapis sadrži veliku količinu informacija koje mogu da se klasifikuju kao osetljive. Uprkos tome, ako je osetljiva informacija prisutna na videu, ali identitet te osobe nije, nema gubitka privatnosti. Isto važi ako se identitet osobe nalazi u video signalu, ali bez osetljivih informacija. U oba slučaja privatnost je zaštićena zato jer osetljive informacije ne mogu da se pridruže nečijem identitetu.

Druga značajna stvar vezana za vizuelnu privatnost je koja osetljiva informacija ili područje od interesa treba da bude obuhvaćeno zaštitom. U dosta slučajeva je lice prikriveno, ali to nije dovoljno da zaštiti vizuelnu privatnost. Čak i ukoliko je lice neke osobe prikriveno drugi elementi koji postoje na slici mogu da ukažu na identifikaciju osobe, na primer prethodno znanje o odeći, visina, hod. Ti elementi mogu da utiču na izbor područja od interesa koja treba da se zaštite, pri čemu tih područja može biti više.

Postoji više različitih metoda za zaštitu privatnosti osoba koje se pojavljuju na video zapisima i slikama. Dva pristupa se pri tome koriste kada se uzima u obzir vremenski aspekt kada se koristi metod zaštite i to pre nego što se snimi slika i posle toga. Sa jedne strane, moguća je prevencija snimanja slika na kojima se pojavljuje neka osoba. Sa druge strane, ako već postoji neka slika koja sadrži osetljive ili privatne informacije kao što su lice, registarska tablica, moguće je njihovo uklanjanje [6]. Neki metodi za zaštitu privatnosti na sekvencama slika su pokazani na Slici 1. U prvoj koloni su prikazane osetljive informacije ili područja od interesa. Druga kolona sadrži područja od interesa koja su zamenjena sa siluetama. U trećoj koloni se nalaze skremblovane osetljive informacije, dok su u poslednjoj koloni inteligentno uklonjena osetljiva područja.

Slika 1. *Neke metode za zaštitu sekvence slika [1]*

U odnosu na to kako je zaštićena privatnost metodi za zaštitu mogu da se podele na sledeći način:

- intervencija;
- slepa (*blind*) vizija;
- bezbedna obrada informacija;
- modifikacija slike i videa, i
- skrivanje podataka [7].

Metode intervencije se odnose na problem prevencije da neko snimi privatne vizuelne podatke iz okruženja. Njihov cilj je da formiraju prostor otporan na snimanja. Ove metode fizički intervenišu na kamerama kako bi se obavila prevencija snimanja slike pomoću specijalizovanog uređaja koji ima spregu sa optičkim sočivom kamere. Metode intervencije su pogodne kada nije moguća dalja kontrola nad već snimljenim slikama. Na primer, aplikacija instalirana na smart telefonima može da bude odgovorna za prevenciju nedozvoljenog snimanja umetničkih dela u muzejima, ukoliko telefon dođe u opseg blutut predajnika. Može se reći da je neophodna nova legislativa u pogledu privatnosti koja obavezuje proizvođače kamera da budu u skladu sa protokolima privatnosti.

Slepa vizija se odnosi na obradu slike i video signala, kao što su detekcija lica, praćenje objekata ili segmentacija slike, na anoniman način.

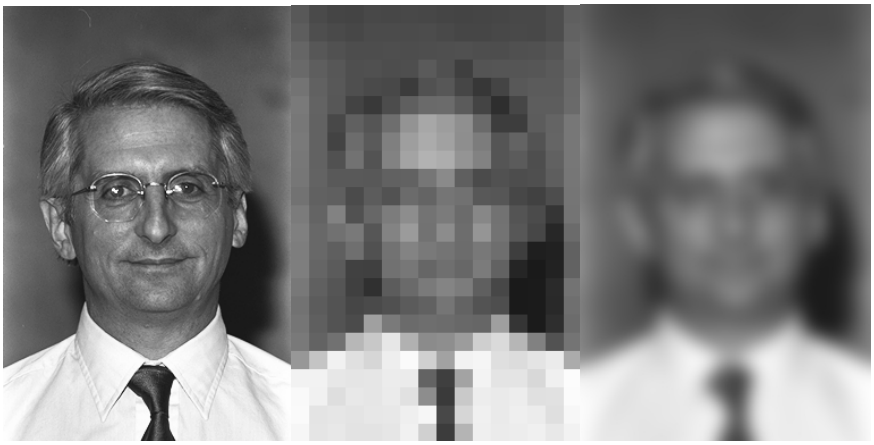
Bezbedna obrada informacija obuhvata metode koji obrađuju vizuelne informacije na način koji zadovoljava privatnost. Na primer, to može da bude algoritam koji obavlja pretraživanje slika u frekvencijskom domenu i ne sadrži vizuelne informacije. U tom slučaju sve slike iz baze podataka koje se pretražuju se konvertuju najpre u frekvencijski domen. Drugi algoritam koristi siluete detektovanih objekata kako bi se analizirala njihova aktivnost.

Modifikacija slike i video signala se odnosi na najčešće korišćene metode za zaštitu vizuelne privatnosti. Te metode modifikuju osetljiva područja na slikama, kao što su lica, tela, registarske tablice, koje sadrže privatne informacije subjekata koji se nalaze na njima. Pri tome se koriste algoritmi računarske vizije kako bi se odredila privatnost osetljivih područja. Imajući u vidu način kako se slika modifikuje metodi modifikacije mogu da se podele na nekoliko kategorija. Najpre, treba pomenuti metode za *ad hoc* distorziju, koje modifikuju područje od interesa na slici bilo kompletnim uklanjanjem osetljivih informacija sa slika, bilo modifikacijom informacija korišćenjem filtara, kao što su to pikselizacija ili zamagljivanje (*blurring*). Slika 2 pokazuje primer za de-identifikaciju originalne slike lica (levo) putem pikselizacije (sredina) i zamagljivanja (desno). Korišćenjem odgovarajućih filtara osetljiva područja se modifikuju tako da onda budu neprepoznatljiva.

Veću robusnost pokazuju metode kao što je kriptovanje slika, čime se privatno osetljivo područje zaključava pomoću ključa. Tehnike kriptovanja se zasnivaju na skremblovanju (permutaciji), koje se koristi i kod analognog video zapisa [8, 9].

Drugi pristup za modifikaciju slike jeste de-identifikacija lica, koja je usmerena ka licima koja se pojavljuju na slikama. Pri tome se najčešće koristi familija algoritama poznata pod nazivom *k-same*, koja implementira *k-anonimnost* model zaštite. Ti algoritmi menjaju lice osobe na način da identitet ne može da se prepozna, ali izrazi lica ostaju očuvani [10].

Neki pristupi, kao što je uklanjanje objekata, koriste inteligentno uklanjanje osetljivih područja tako što popunjavaju nastalu prazninu sa odgovarajućom pozadinom.



Slika 2. *De-identifikacija lica pikselizacijom i zamagljivanjem [8]*

4. Mere pravne zaštite

Dok ovaj rad nastaje digitalni svet se uzburkao zbog sporazuma koji je bio na snazi već 15 godina i koji je omogućavao vlastima Sjedinjenih Američkih Država (u daljem tekstu SAD) rutinski pristup podacima o stanovnicima Evrope. U pitanju je Sporazum **„Sigurna luka" (*„Safe Harbor"*)** koji su 2000. godine SAD potpisale sa Evropskom unijom (u daljem tekstu EU) i koji od 6-og oktobra 2015. godine prema odluci Evropskog Suda pravde iz Luksemburga više ne važi, jer ne garantuje dovoljnu zaštitu korisničkih podataka Evropljana [11].

Generalni advokat Evropskog Suda pravde mišljenje je zasnovao na konstatacijama da su Uprava za nacionalnu bezbednost i druge bezbednosne agencije SAD u mogućnosti da pristupaju prenesenim ličnim podacima na "masovan i neselektivan način" što ugrožava pravo na privatnost po članu sedam Povelje o osnovnim pravima EU. Ovo mišljenje je zasnovano i na stavu da građani EU "nemaju odgovarajući pravni lek protiv obrade svojih ličnih podataka prenetih u SAD u druge svrhe osim onih u koje su prvobitno prikupljeni".

Evropski Sud odlučio je da organi za zaštitu podataka u svakoj od 28 zemalja članica EU imaju pravo da procenjuju kako se iznose podaci u SAD i moći će da nametnu strože sankcije za određene transfere podataka. Presuda je od značaja i za Srbiju, iako naša zemlja nije članica EU, kako je saopšteno iz kabineta Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti i ova odluka će imati globalne posledice. Inače, Srbija ima obavezu da svojim građanima i rezidentima obezbedi prava na zaštitu podataka o ličnosti zajamčena Ustavom, zakonom i Konvencijom 108. Saveta Evrope. *(Videti: Zakon o potvrđivanju Konvencije o zaštiti lica u odnosu na automatsku obradu ličnih podataka, "Sl. list SRJ - Međunarodni ugovori", br. 1/92, "Sl. list SCG – Međunarodni ugovori", br. 11/2005 i "Sl. glasnik RS - Međunarodni ugovori", br.98/2008 i 12/2010.)*

U Republici Srbiji postoji veći broj propisa koji su posvećeni zaštiti privatnosti i sankcionišu ugrožavanje i narušavanje privatnosti drugih lica.

Zakonom o zaštiti podataka o ličnosti *("Sl. glasnik RS" br. 97/08, 104/09, 68/12, 107/12*) uređuju se uslovi za prikupljanje i obradu podataka o ličnosti, prava lica i zaštita prava lica čiji se podaci prikupljaju i obrađuju, ograničenja zaštite podataka o ličnosti, postupak pred nadležnim organom za zaštitu podataka o ličnosti, obezbeđenje podataka, evidencija, iznošenje podataka iz Republike Srbije i nadzor nad izvršavanjem ovog zakona (član 1. stav 1). Ovim zakonom propisano je da podaci moraju biti odgovarajuće zaštićeni od zloupotreba, uništenja, gubitka, neovlašćenih promena ili pristupa. (član 47. Zakona).

U skladu sa **Zakonom o elektronskim komunikacijama** *("Sl. glasnik RS" br. 44/10, 60/13, 62/14*) ciljevi i načela regulisanja odnosa u oblasti elektronskih komunikacija zasnivaju se i na obezbeđivanju visokog nivoa zaštite podataka o ličnosti i privatnosti korisnika, a u skladu sa Zakonom o zaštiti podataka o ličnosti i drugim zakonima (član 3. Zakona).

U skladu sa članom 80. **Zakona o javnom informisanju i medijima** ***("****Sl. glasnik RS" br. 83/14, 58/15)* informacija iz privatnog života, odnosno lični zapis (pismo, dnevnik, zabeleška, digitalni zapis i sl.), zapis lika (fotografski, crtani, filmski, video, digitalni i sl.) i zapis govora (magnetofonski, gramofonski, digitalni i sl.), ne može se objaviti bez pristanka lica čijeg se privatnog života informacija tiče, odnosno lica čije reči, lik odnosno glas sadrži, ako se pri objavljivanju može zaključiti koje je to lice.

Krivični zakonik Republike Srbije *("Sl. glasnik RS" br. 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13, 108/14*) predviđa u članu 144. krivično delo neovlašćeno fotografisanje prema kome "ko neovlašćeno načini fotografski, filmski, video ili drugi snimak nekog lica i time osetno zadre u njegov lični život ili ko takav snimak preda ili pokazuje trećem licu ili mu na drugi način omogući da se sa njim upozna, kazniće se novčanom kaznom ili zatvorom do jedne godine", dok član 145. reguliše krivično delo neovlašćeno objavljivanje i prikazivanje tuđeg spisa, portreta i snimka, pa će se ko objavi ili prikaže spis, portret, fotografiju, film ili fonogram ličnog karaktera bez pristanka lica koje je spis sastavilo ili na koga se spis odnosi, odnosno bez pristanka lica koje je prikazano na portretu, fotografiji ili filmu ili čiji je glas snimljen na fonogramu ili bez pristanka drugog lica čiji se pristanak po zakonu traži i time osetno zadre u lični život tog lica, kazniti novčanom kaznom ili zatvorom do dve godine.

Manji broj propisa u Republici Srbiji dozvoljava određeni stepen ugrožavanja privatnosti koji zakonodavac pravda višim ciljevima.

Zakon o bezbednosti saobraćaja na putevima *("Sl. glasnik RS" br. 41/09, 53/10, 101/11, 32/13, 55/14*) među posebnim merama i ovlašćenjima koja se preduzimaju radi sprečavanja ugrožavanja bezbednosti učesnika u saobraćaju, odnosno omogućavanja odvijanja saobraćaja u članu 278. predviđa i snimanje saobraćaja i učesnika u saobraćaju korišćenjem odgovarajućih sredstava kao i dokumentovanje prekršaja i drugih delikta u saobraćaju.

Zakonom o sprečavanju nasilja i nedoličnog ponašanja na sportskim priredbama *("Sl. glasnik RS" br. 67/03, 101/05, 90/07, 72/09, 111/09, 104/13)* u članu 15. propisana je dužnost organizatora da obezbedi da se sportska priredba povećanog rizika održi u sportskom objektu koji ima i tehničku opremu za praćenje i snimanje ulaska i ponašanja gledalaca na sportskom objektu.

Zakonik o krivičnom postupku *("Sl. glasnik RS" br. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14*) dozvoljava da na obrazloženi predlog javnog tužioca sud može odrediti

tajno praćenje i snimanje osumnjičenog radi: 1) otkrivanja kontakata ili komunikacije osumnjičenog na javnim mestima i mestima na kojima je pristup ograničen ili u prostorijama, osim u stanu, (a ova mesta ili prostorije, odnosno prevozna sredstva drugih lica mogu biti predmet tajnog nadzora i snimanja samo ako je verovatno da će osumnjičeni tu biti prisutan ili da koristi ta prevozna sredstva); kao i 2) utvrđivanja istovetnosti lica ili lociranja lica ili stvari. (Videti: član 171. Zakonika) Tajno praćenje i snimanje može trajati tri meseca, a zbog neophodnosti daljeg prikupljanja dokaza može se produžiti najviše za tri meseca, dok ga izvršava policija, Bezbednosno-informativna agencija ili Vojnobezbednosna agencija.

Zakonom o policiji *("Sl. glasnik RS" br. 101/05, 63/09, 92/11, 64/15*) među policijskim ovlašćenjima utvrđenim ovim Zakonom predviđeno je i snimanje na javnim mestima (član 30. Zakona). Snimanje na javnim mestima definisano je ovim zakonom kao trajni akustički i video nadzor javnih mesta na kojima se učestalo vrše krivična dela ili prekršaji, radi njihovog sprečavanja. Prema članu 69. ovog zakona kada postoji opasnost da prilikom javnog okupljanja dođe do ugrožavanja života i zdravlja ljudi ili imovine, ovlašćeno službeno lice ovlašćeno je da vrši video snimanje ili fotografisanje javnog skupa, ali nameru da sprovede napred navedene aktivnosti policija mora javno da saopšti.

Zakonom o komunalnoj policiji *("Sl. glasnik RS" br. 51/09*) propisano je da kada je to potrebno radi sprečavanja kršenja propisa iz delokruga komunalne policije, određeni prostor i objekat može se obezbediti video nadzorom, dok uređaji za video nadzor moraju biti vidljivi, sa istaknutim natpisom da je prostor ili objekat obezbeđen video nadzorom. (član 23. Zakona).

Prema **Zakonu o privatnom obezbeđenju** *("Sl. glasnik RS" br. 104/13, 42/15*) kada se poslovi zaštite objekta ili prostora koji se koriste za javnu upotrebu vrše uz upotrebu uređaja za snimanje slike, pravno lice i preduzetnik za privatno obezbeđenje dužni su da na vidljivom mestu istaknu obaveštenje da je objekat ili prostor zaštićen video obezbeđenjem, a korisnik usluga je obavezan da to prihvati i arhivirane snimke čuva najmanje 30 dana i da ih, na zahtev, stavi na uvid ovlašćenom policijskom službeniku. Ovi podaci, kao i podaci koji su prikupljeni u vršenju posla privatnog obezbeđenja mogu se koristiti samo u svrhu za koju su prikupljeni i zabranjeno je njihovo ustupanje trećim licima i javno objavljivanje, osim u slučajevima predviđenim zakonom, odnosno ugovorom. (članovi 32. i 68. Zakona).

Srbija još nije adekvatnim propisom regulisala ni upotrebu dronova, dok su Amerikanci to uradili, upravo posle nedavnog incidenta u Beogradu 2014. godine. Federalna uprava za avijaciju (FAA) zabranila je letove dronova i sličnih bespilotnih letelica u blizini stadiona u SAD i najavila jednogodišnju kaznu zatvora za sve koji budu kršili zakon [12]. Zabrana se odnosi na oko 150 stadiona koji mogu da prime 30.000 i više gledalaca, a doneta je zbog zabrinutosti da bi ove letelice mogle da se sruše u publiku što bi moglo imati tragične posledice.

Iz Direktorata civilnog vazduhoplovstva Srbije saopšteno je da bi „na predlog ministra nadležnog za saobraćaj Vlada Srbije trebalo da donese propis koji će određivati uslove pod kojima se lansiraju dronovi". U sadašnjim zakonskim okvirima, Direktorat se ne smatra nadležnim za dronove, jer ne spadaju u vazduhoplove, a u smislu Zakona o vazdušnom saobraćaju (*"Službeni glasnik RS", br. 73/2010, 57/2011.)* dron se može smatrati „letećim objektom" koji se mogu lansirati u privredne, naučne, sportske i druge

svrhe, tako da ne ugrožavaju bezbednost vazdušnog saobraćaja. Za eventualnu štetu koja je nastala usled lansiranja letećih objekata odgovorno je lice koje je raketu, odnosno drugi leteći objekat, lansiralo. Za snimanje iz vazduha i u našoj zemlji uveliko se koriste dronovi (poznati su efektni snimci majskih poplava 2014. godine snimljenih iz drona), ali je za to potrebno dobiti odobrenje Ministarstva odbrane.

Očigledno je da se važeći zakoni i propisi, koji bi se u izvesnoj meri mogli odnositi i na dronove, moraju menjati i usvajati novi, jer su neki od njih doneti davno pre nego što su se ove letelice pojavile i u međuvremenu postale masovno dostupne. I dok u Srbiji nema najave donošenja novih propisa, u SAD se radi na novim propisima, uključujući i upotrebu dronova u komercijalne svrhe – za nadzor iz vazduha, izradu mapa, praćenje života u divljini, obavljanje nekih opasnih ili poslova u zabačenim oblastima...

5. Zaključak

Sveprisutnost društvenih mreža, zastupljenost kamera za video nadzor na javnim mestima, kao i razvoj multimedijalnih komunikacija, doprineli su da privatnost korisnika u savremenom društvu bude dovedena u pitanje. Novi servisi i alati bi morali da uzmu u obzir pravo na privatnost. U ovom radu dat je pregled metoda za zaštitu vizuelne privatnosti. Od metoda su opisane intervencija nad multimedijalnim sadržajima, slepa vizija, bezbedna obrada, modifikacija slike i videa, kao i skrivanje podataka. Akcenat je stavljen na metode modifikacije, koje obuhvataju filtriranje slike, kriptovanje, de-identifikaciju lica, kao i uklanjanje objekata.

Od pravnih propisa očekuju se određena rešenja, a zaštita privatnosti u sferi video nadzora je oblast u kojoj pravni propisi tek treba da se uobliče. Nedavno doneta presuda Evropskog suda pravde kojom je utvrđeno da je nevažeći sporazum "Sigurna luka" između EU i SAD, a na osnovu kojeg su podaci o ličnosti bez posebnih formalnosti i odobrenja transferisani u SAD, predstavlja jedan od najvažnijih presedana u dosadašnjoj međunarodno-pravnoj praksi zaštite podataka o ličnosti. Verujemo da će nam ovaj obrt na relaciji EU-SAD povodom obrade odnosno zaštite podataka o ličnosti pomoći da bolje sagledamo nedorečenost i nedostatke naših pravnih rešenja u vezi sa iznošenjem podataka o ličnosti u inostranstvo.

Literatura

[1] J.R. Padilla-Lopez, A.A. Chaaraoui, F. Florez-Revuelta: „Visual privacy protection: a survey“, *Expert Systems with Applications*, Vol. 42, No. 9, pp 4177-4195, 2015.

[2] G. Friedland, A. Janin, H. Lei, J. Choi, R. Sommer: „Content-based privacy for consumer-produced multimedia“, in *Multimedia Data Mining and Analytics*, Springer International Publishing, pp 157-173, 2015.

[3] T. Winkler, B. Rinner: „User-centric privacy awareness in video surveillance“, *Multimedia Systems*, Vol. 18, No. 2, pp 99-121, 2012.

[4] A. Senior, S. Pankanti: „Privacy Protection and Face Recognition“, in *Handbook of Face Recognition*, Springer: London, UK, pp 671–691, 2011.

[5] M. Piccardi: „Background subtraction techniques: a review“, *Proceedings of the* 2004 *IEEE International Conference on Systems, Man and Cybernetics*, The Hague, The Netherlands, Vol. 4, pp 3099–3104, 10–13. October 2004.

[6] L. Du, L. Haibin: „Preservative license plate de-identification for privacy protection“, IEEE *International Conference on Document Analysis and Recognition ICDAR,* 2011.
[7] F. Petitcolas, R. Anderson, M. Kuhn: „Information hiding - a survey“, *Proceedings of* IEEE, Vol. 87, pp 1062–1078, 1999.
[8] P. Korshunov, T. Ebrahimi: „Scrambling-based tool for secure protection of JPEG images“, *IEEE International Conference on Image Processing (ICIP),* 2014.
[9] S. Cimato, C.N. Yang, eds. *Visual cryptography and secret image sharing*, CRC press, 2011.
[10] L. Sweeney: „k-anonymity: a model for protecting privacy“, *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, Vol. 10, No. 5, pp 557-570, 2002.
[11] Donnees personnelles: l' après – Safe Harbor, “Le Monde“ 8.10. 2015, p. 8.
[12] M. Bonetto, P. Korshunov, G. Ramponi, T. Ebrahimi: „Privacy in mini-drone based video surveillance“, *Workshop on De-identification for privacy protection in multimedia*, No. EPFL-CONF-206109, 2015.

Abstract: *The right to privacy has for a long time been one of the basic human rights. In the last thirty years the development of information and communication technologies has led to rapid progress in collecting, storing, transferring and sharing of personal information in the public and private sector. The combination of universal sensors, wireless communication and pattern recognition has made easier than ever observation of our daily activities. On the other hand, the use of video surveillance, social networks and personal information, led to doubts in respect of the further use of the collected data. In order to reduce the concern we need to develop effective mechanisms regarding the privacy protection of visual information.*

Keywords: *privacy protection, video surveillance, image processing, social networks, legal protection*

PRIVACY PROTECTION ON VISUAL INFORMATION IN NETWORKED WORLD

Andreja Samčović, Nataša Tomić - Petrović